PATENT ABSTRACTS OF JAPAN

(11) Publication number : 09-152990
(43) Date of publication of application : 10.06.1997

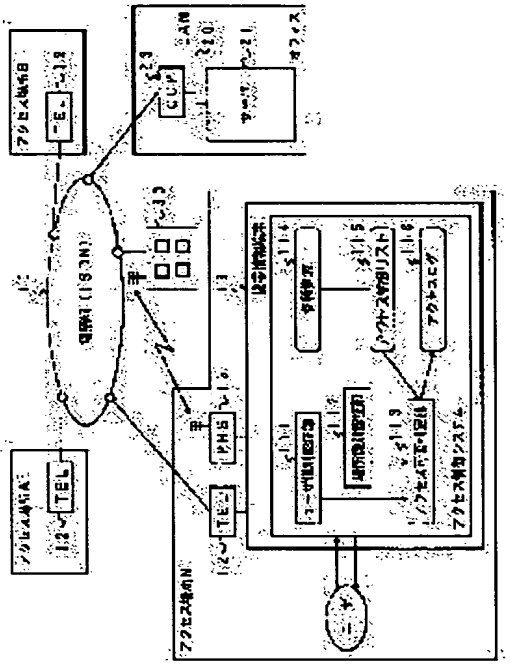
(51) Int.Cl. G06F 12/14
G06F 12/14
G06F 12/00
G06F 15/00

(21) Application number : 07-312592
(22) Date of filing : 30.11.1995

(71) Applicant : TOSHIBA CORP
(72) Inventor : YOSHINO YASUAKI

(54) ACCESS CONTROL SYSTEM AND ITS METHOD

(57) Abstract:
PROBLEM TO BE SOLVED: To attain an access control system for obtaining security optimum to a mobile computing environment.
SOLUTION: An access place for utilizing an information terminal 11 is specified by a place identifying/certificating part 112 and an access control list 115 is searched by the specified information security level. An information security level necessary for accessing each resource is regulated in the list 115. Consequently, an access place requested by a user can be added to an access availability judging reference and restriction to resources to be utilized can be changed in accordance with the access place.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－152990

(43)公開日　平成９年(1997)６月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３１０		Ｇ０６Ｆ	12/14	３１０Ｋ
		３２０				３２０Ａ
	12/00	５３７			12/00	５３７Ａ
	15/00	３３０			15/00	３３０Ｄ

審査請求　未請求　請求項の数９　ＯＬ　（全 16 頁）

(21)出願番号　特願平7－312592

(22)出願日　平成７年(1995)11月30日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　吉野　恭明
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

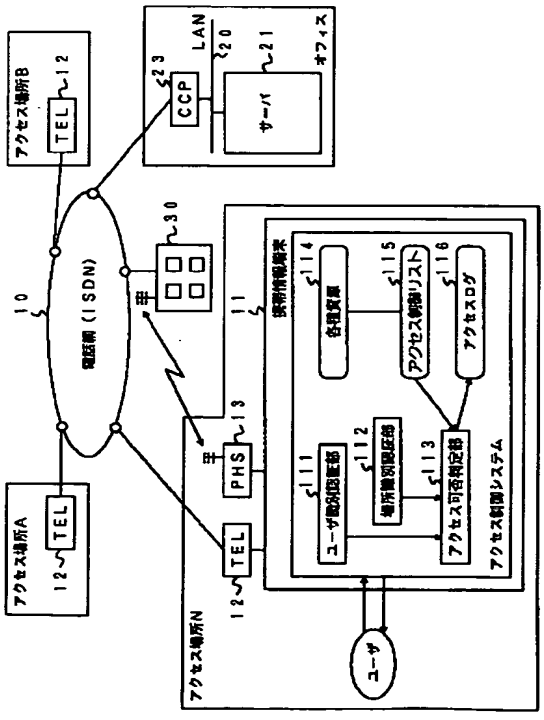
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　アクセス制御システムおよびアクセス制御方法

(57)【要約】

【課題】モーバイルコンピューティング環境に最適なセキュリティー確保のためのアクセス制御システムを実現する。

【解決手段】情報端末１１を利用するアクセス場所が場所識別認証部１１２によって特定され、その特定された情報セキュリティーレベルを用いて、アクセス制御リスト１１５がサーチされる。アクセス制御リスト１１５には、資源毎にそれをアクセスするために必要な情報セキュリティーレベルが規定されている。従って、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。



1

【特許請求の範囲】

【請求項１】　各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、

前記資源のアクセスのために利用者によって情報端末が使用されるアクセス場所を特定するアクセス場所特定手段と、

このアクセス場所特定手段によって特定されたアクセス場所に対して予め設定されている情報セキュリティーレベルに応じて、前記利用者から要求された資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備することを特徴とするアクセス制御システム。

【請求項２】　前記アクセス可否判定手段は、

各資源とその資源をアクセスするために必要なアクセス場所の情報セキュリティーレベルとの対応関係を規定したアクセス制御リストを有し、

このアクセス制御リストの内容と、前記アクセス場所特定手段によって特定されたアクセス場所の情報セキュリティーレベルとに従って、前記利用者から要求された資源に対するアクセスの可否を判定することを特徴とする請求項１記載のアクセス制御システム。

【請求項３】　前記アクセス場所特定手段は、

利用者によって情報端末が使用されるアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従ってアクセス場所を特定することを特徴とする請求項１記載のアクセス制御システム。

【請求項４】　前記通信装置は、

その通信装置が設置されているアクセス場所を示す識別子を暗号化して発生し、

前記情報セキュリティーレベル検出手段は、前記暗号化された識別子を復号化して前記アクセス場所を特定することを特徴とする請求項３記載のアクセス制御システム。

【請求項５】　携帯情報端末を用いたモーバイルコンピューティング環境下で、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティーレベルを検出する情報セキュリティーレベル検出手段と、

各資源とその資源をアクセスするために必要な情報セキュリティーレベルとの対応関係を規定したアクセス制御リストと、前記情報セキュリティーレベル検出手段によって検出された前記アクセス場所の情報セキュリティーレベルとに従って、前記利用者から要求された前記携帯情報端末内の資源、または前記携帯情報端末と通信媒体を介して接続可能な他の情報処理装置内の資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備することを特徴とするアクセス制御システム。

2

【請求項６】　携帯情報端末と、通信媒体を介して前記携帯情報端末と各種情報を授受するサーバ計算機とを利用したモーバイルコンピューティング環境下で、前記サーバ計算機内の各種コンピュータ資源に対する前記携帯情報端末の利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、

前記携帯情報端末は、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティーレベルを検出する情報セキュリティーレベル検出手段を具備し、

前記サーバ計算機は、

各資源とその資源をアクセスするために必要な情報セキュリティーレベルとの対応関係を規定したアクセス制御リストを保持する手段と、

前記携帯情報端末の前記情報セキュリティーレベル検出手段によって検出された前記アクセス場所の情報セキュリティーレベルと、前記アクセス制御リストとに従って、前記携帯情報端末から要求された前記サーバ計算機内の資源に対するアクセス要求の可否を判定する手段とを具備することを特徴とするアクセス制御システム。

【請求項７】　携帯情報端末と、通信媒体を介して前記携帯情報端末と各種情報を授受するサーバ計算機とを利用したモーバイルコンピューティング環境下で、前記サーバ計算機内の各種コンピュータ資源に対する前記携帯情報端末の利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、

前記携帯情報端末は、

前記サーバ計算機から提供された資源を保持し、その運用および管理を行うキャッシュ管理手段と、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティーレベルを検出する情報セキュリティーレベル検出手段と、

各資源とその資源をアクセスするために必要な情報セキュリティーレベルとの対応関係を規定したアクセス制御リストと、前記情報セキュリティーレベル検出手段によって検出された前記アクセス場所の情報セキュリティーレベルとに従って、前記利用者から要求された前記キャッシュ管理装置内の資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備し、

前記サーバ計算機は、

各資源とその資源をアクセスするために必要な情報セキュリティーレベルとの対応関係を規定したアクセス制御リストを保持する手段と、

前記携帯情報端末の前記情報セキュリティーレベル検出手段によって検出された前記アクセス場所の情報セキュ

リティーレベルと、前記アクセス制御リストとに従って、前記携帯情報端末から要求された前記キャッシュ管理部に存在していない前記サーバ計算機内の資源に対するアクセス要求の可否を判定する手段とを具備することを特徴とするアクセス制御システム。

【請求項８】　携帯情報端末を用いたモーバイルコンピューティング環境下で、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御方法において、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所の情報セキュリティーレベルを検出し、

この検出された前記アクセス場所の情報セキュリティーレベルに従って、前記利用者から要求された資源に対するアクセスの可否を判定し、

アクセス場所に応じて利用可能な資源を制限することを特徴とするアクセス制御方法。

【請求項９】　携帯情報端末を用いたモーバイルコンピューティング環境下で、利用者が前記携帯情報端末を用いてアクセス操作を行うアクセス場所に応じて、前記携帯情報端末の利用者からのコンピュータ資源に対するアクセス要求を許可または禁止するアクセス制御方法であって、

前記携帯情報端末が利用されるアクセス場所毎にそのアクセス場所に対応する情報セキュリティーレベルを示す電波環境を提供し、

その電波環境下におかれた前記携帯情報端末がその電波を受信することによって、その携帯情報端末が利用されるアクセス場所の情報セキュリティーレベルを検出し、

その検出された情報セキュリティーレベルを用いることにより、アクセス場所に応じて利用可能な資源を制限できるようにしたことを特徴とするアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムおよびアクセス制御方法に関する。

【０００２】

【従来の技術】近年、コンピュータやネットワーク技術の発達、あるいはそれらを利用した情報サービスの発展に伴い、様々な情報セキュリティー技術が実現されている。この情報セキュリティーを実現する技術の１つとして、アクセス制御が知られている。

【０００３】アクセス制御とは、ユーザ認証などにより識別された主体から要求されたコンピュータ資源へのアクセスを、予め設定されたアクセス制御リストを用いて許可するか禁止するかの制御を行う技術をいう。アクセス制御リストには、ユーザ名とそのユーザが利用可能な資源との対応関係などが記述されている。

【０００４】このアクセス制御技術を利用することにより、特定個人／特定計算機の関係において特定資源の利用だけを許可するという情報セキュリティーが実現され、悪意を持った様々な不正アクセスからコンピュータ資源を保護することができる。

【０００５】しかし、ＰＤＡ、サブノートＰＣ等の携帯情報端末を用いるモーバイルコンピューティング環境下においては、個人や計算機の情報だけでアクセス可否を判断する従来のアクセス制御技術では、十分な情報セキュリティーを得ることはできない。

【０００６】すなわち、モーバイルコンピューティング環境下では、個人が携帯情報端末を持ち歩いて、不特定の場所からその携帯情報端末内のデータを直接アクセスしたり、遠隔地にあるサーバ計算機のデータベースなどにネットワーク経由でアクセスする可能性がある。この場合、その携帯情報端末が使用される場所によっては、サーバから提供された機密性を持つ情報や個人認証のためのパスワードが第三者に盗まれたり、その情報漏洩が元で、ネットワークを介したサーバ計算機への不正進入を許し、機密情報の改竄や運用妨害といった攻撃を受ける危険がある。

【０００７】また、最近では、携帯情報端末自体から発生される電磁波から、その携帯情報端末の表示画面の内容や操作状況を読みとることができるという報告もなされている。したがって、モーバイルコンピューティング環境下では、携帯情報端末を使用する場所そのものが、セキュリティー保持のための重要な要素となっている。

【０００８】

【発明が解決しようとする課題】上述したように、モーバイルコンピューティング環境下では、個人が携帯情報端末を持ち歩いて、不特定の場所からその携帯情報端末内のデータを直接アクセスしたり、遠隔地にあるサーバ計算機のデータベースなどにネットワーク経由でアクセスする可能性があるため、個人や計算機の情報だけでアクセス可否を判断する従来のアクセス制御技術では、十分な情報セキュリティーを得ることができないという問題がある。

【０００９】この発明はこの様な点に鑑みてなされたものであり、個人や計算機の情報だけでなく、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようにして、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現し得るアクセス制御システムおよびアクセス制御方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】この発明は、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、前記資源のアクセスのために利用者によって情報端末が使用されるアクセス場所を特定するアクセス場所特定手段と、このアクセス場所特定手段によって特定

されたアクセス場所について予め設定された情報セキュリティーレベルに応じて、前記利用者から要求された資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備することを特徴とする。

【００１１】このアクセス制御システムにおいては、情報端末を利用するアクセス場所が特定され、そのアクセス場所の情報セキュリティーレベルを使用したアクセス制御が行われる。このため、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。

【００１２】従って、公共の場所などのようにセキュリティーレベルが低い場所では機密性の高い情報へのアクセスは禁止されるが、外出先であっても、セキュリティーレベルが高い場所であれば、機密情報にアクセスすることができる。よって、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現できる。

【００１３】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図１には、この発明の一実施形態に係るアクセス制御システムが適用されるモーバイルコンピューティングシステム全体の構成が示されている。このモーバイルコンピューティングシステムは、携帯情報端末１１と、この携帯情報端末１１と電話回線網やＩＳＤＮなどの通信網１０を介して各種情報を授受するサーバ計算機２１とを利用して実現されている。

【００１４】携帯情報端末１１は例えばＰＤＡやノートＰＣ等の小型電子機器であり、自宅、マンション、自社オフィス、サテライトオフィス、貸しオフィス、ホテル、喫茶店、公園、空港、地下鉄など、不特定の場所（アクセス場所Ａ，Ｂ，…，Ｎ）で利用される。この携帯情報端末１１はその端末１１内の記憶装置に対する情報の入出力を始め、通信網１０を経由してサーバ計算機２１をアクセスするための通信機能も有している。携帯情報端末１１の利用者が外出先などからサーバ計算機２１と通信する場合には、その利用者が現在いる場所に設置されている電話機１２等の公衆通信端末に携帯情報端末１１が接続され、有線通信の形態で携帯情報端末１１とサーバ計算機２１間の通信が行われる。また、ＰＨＳ１３等の携帯電話を使用すれば、電話機１２がない場所でも、最寄りの無線電話基地局３０経由でサーバ計算機２１と通信することができる。

【００１５】サーバ計算機２１は、例えばオフィス内等に配置されている計算機であり、ＬＡＮ２０および通信制御装置（ＣＣＰ）２３等を介して通信回線網１０と接続されている。

【００１６】この実施形態では、携帯情報端末１１内に次のようなアクセス制御システムが実現されている。このアクセス制御システムは、携帯情報端末１１内の各種

資源１１４に対する利用者からのアクセス要求を許可または禁止するための制御を行うソフトウェアであり、ユーザ識別認証部１１１、アクセス場所識別認証部１１２、アクセス可否判定部１１３、アクセス制御リスト１１５、およびアクセスログ１１６を備えている。

【００１７】ユーザ識別認証部１１１は、携帯情報端末１１の利用者によって入力されるユーザ名を使用して利用者が誰であるかを識別し、次いで、そのユーザ名に対応する登録パスワードと利用者によって入力されるパスワードとの照合を行って、利用者が正当な人であることを調べるための認証を行う。

【００１８】アクセス場所識別認証部１１２は、携帯情報端末１１が現在利用されているアクセス場所およびそのアクセス場所について予め設定された情報セキュリティーレベルについてその識別および認証を行う。このアクセス場所識別認証部１１２による場所に関する識別および認証処理の原理を図２に示す。

【００１９】図２に示されているように、例えば、貸しオフィス、ホテル、喫茶店、各種交通機関等に構築された各アクセス場所においては、セキュリティーレベル発信器１００が予め設置されており、そのセキュリティーレベル発信器１００から送信される電波等の無線信号が携帯情報端末１１によって受信される。

【００２０】セキュリティーレベル発信器１００から携帯情報端末１１の場所識別認証部１１２に与えられる情報は、そのアクセス場所を特定するための識別子とそのアクセス場所に対して予め設定された情報セキュリティーレベルである。

【００２１】各アクセス場所の情報セキュリティレベルは、公共的な中立機関によって定めた基準に従って決定する。すなわち、中立機関は、アクセス場所毎にそのアクセス場所の環境を評価し、基準に従ってそのアクセス場所の情報セキュリティーレベルを認定する。情報セキュリティーレベルは、セキュリティに関して何も考慮されていない最低レベルから、ソフト／ハード両側面から最大級の対策が施されている最高レベルまで、複数の段階に区分される。これにより、自宅、自社オフィス、サテライトオフィス、貸しオフィス、ホテル、喫茶店、各種交通機関等においては、用途／予算に応じて、様々なセキュリティレベルの「アクセス場所」を構築することができる。

【００２２】情報セキュリティーレベルの認定がなされたアクセス場所に対しては、その場所の識別子と認定された情報セキュリティーレベルの情報とが設定されたセキュリティーレベル発信器１００が付与される。

【００２３】この場合、セキュリティーレベル発信器１００から発生される情報の改竄を防止するために、セキュリティーレベル発信器１００に設定される情報は中立機関によって電子署名などの暗号技術を用いて暗号化されて保護されている。従って、セキュリティーレベル発

信器１００からも暗号化された信号が発生されることになる。携帯情報端末１１は、この暗号化された信号を復号化してアクセス場所の識別子および情報セキュリティレベルを認識する。

【００２４】図３には、セキュリティーレベル発信器１００から発生されるセキュリティーレベル信号の内容とセキュリティレベルの高低との対応関係が示されている。この例では、セキュリティーレベル信号Ａが最もセキュリティーが高く、セキュリティーレベル信号Ｂ，Ｃ，Ｄ，Ｅ，Ｆの順でセキュリティーレベルが段階的に低くなる。また、場所識別子や情報セキュリティーレベルについての情報が得られない場所は、場所不明、且つ最低レベルのセキュリティとして扱われる。

【００２５】以上のように、場所識別認証部１１２は、携帯情報端末１１が存在するアクセス場所の電波環境からその場所とその場所の情報セキュリティーレベルを決定する。

【００２６】次に、図１のアクセス制御システムの他の構成要素について説明する。アクセス可否判定部１１３は、ユーザ識別認証部１１１および場所識別認証部１１２それぞれからの識別認識情報と、アクセス制御リスト１１５の内容に従って、ユーザから要求された資源に対するアクセスを許可するか否かの可否判定を行う。この判定結果は、アクセス制御の履歴情報としてアクセスログ１１６に記録される。この履歴情報は、攻撃行為の検出や攻撃者の特定などに使用される。

【００２７】アクセス制御リスト１１５は、各種資源１１４それぞれについて、それをアクセス可能なユーザ名（またはグループ名）とアクセス場所の情報セキュリティーレベルを規定したものであり、図４に示されているように、資源、ユーザ名（またはグループ名）、および情報セキュリティーレベルの対応関係が保持されている。この図４の例では、データファイルＡをアクセスするために必要なアクセス場所の情報セキュリティーレベルは“Ａ”であり、データファイルＢをアクセスするために必要なアクセス場所の情報セキュリティーレベルは“Ｃ”である場合が示されている。この場合、もしデータファイルＡ，Ｂ双方についてアクセスが許可されている利用者が、携帯情報端末１１を情報セキュリティーレベル“Ｂ”のアクセス場所で操作すると、データファイルＢに対するアクセス要求については許可されるが、データファイルＡに対するアクセス要求については禁止される。

【００２８】次に、図５のフローチャートを参照して、図１のアクセス制御システムの動作について説明する。ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。

【００２９】１．アクセス制御システムは、ユーザがある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップＳ１１）、以下のアクセス制御動作を行う。

【００３０】２．すなわち、まず、アクセス制御システムのユーザ識別認証部１１１は、ユーザを特定し、場所識別認証部１１２はユーザのいる場所の情報セキュリティレベルを特定して、結果をアクセス可否判定部１１３に渡す（ステップＳ１２，１３）。

【００３１】３．次に、アクセス可否判定部１１３は、ユーザ、アクセス場所の情報セキュリティレベル、およびアクセス対象資源の情報を元にアクセス制御リスト１１５をサーチし、アクセス要求の許可／非許可の判定を行う（ステップＳ１４）。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ１１６に記録される（ステップＳ１５，１６）。

【００３２】４．また、アクセス要求を許可した場合には、アクセス制御システムは、ユーザに対して要求された資源を渡す（ステップＳ１７）。以上のように、この実施形態１においては、情報端末１１を利用するアクセス場所が特定され、そのアクセス場所の情報セキュリティーレベルを使用したアクセス制御が行われる。このため、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。

【００３３】従って、公共の場所などのようにセキュリティーレベルが低い場所では機密性の高い情報へのアクセスは禁止されるが、外出先であっても、セキュリティーレベルが高い場所であれば、機密情報にアクセスすることができる。よって、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現できる。

【００３４】次に、図６乃至図８を参照して、この発明の第２実施形態を説明する。図６には、この発明の第２実施形態に係るアクセス制御システムの実現形態が示されている。第２実施形態のアクセス制御システムは、携帯情報端末１１が存在するアクセス場所の情報セキュリティーレベルを使用したアクセス制御を行う点については実施形態１と同様であるが、ここでは、携帯情報端末１１がサーバ計算機２１内の各種資源２１５に対するアクセスを要求し、そのアクセス可否判定をサーバ計算機２１内で行うように構成されている。

【００３５】すなわち、アクセス制御システムを実現するための構成要素のうち、携帯情報端末１１側には、ユーザ識別認証部１２１およびアクセス場所識別認証部１２２が設けられており、サーバ計算機２１側には、ユーザ情報検証部２１１、計算機識別認証部２１２、場所情報検証部２１３、アクセス可否判定部２１４、アクセス制御リスト２１６、およびアクセスログ２１７が設けられている。

【００３６】次に、図７および図８のフローチャートを

参照して、図６のアクセス制御システムの動作について説明する。ここで、図７は携帯情報端末１１側の処理を示し、図８はサーバ計算機２１側の処理を示している。

【００３７】ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。

１．携帯情報端末１１のアクセス制御システムは、ユーザがサーバ計算機２１内のある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップＳ２１）、以下のアクセス制御動作を行う。

【００３８】２．すなわち、まず、携帯情報端末１１のユーザ識別認証部１２１はユーザを特定し、場所識別認証部１２２はユーザのいる場所のセキュリティレベルを特定する。そして、それらの情報を、アクセス要求された対象資源情報とともに、リモートマシンであるサーバ計算機２１にアクセス要求として送る（ステップＳ２４）。

【００３９】３．サーバ計算機２１はそのアクセス要求に応答してイベント待ち状態から抜け（ステップＳ３１）、そして、計算機識別認証部２１２は、要求元の計算機を特定し、結果をアクセス可否判定部２１４に渡す（ステップＳ３２）。また、ユーザ情報検証部２１１と場所情報検証部２１２は、携帯情報端末１１から送られてきた情報が正しいかを検証し、結果をアクセス可否判定部２１４に渡す（ステップＳ３３，Ｓ３４）。

【００４０】４．アクセス可否判定部２１４は、ユーザ、アクセス場所のセキュリティレベル、要求元の計算機、対象資源の情報を元に、アクセス制御リスト２１６をサーチし、アクセス要求の許可／非許可を判定する（ステップＳ３５）。アクセス制御リスト２１６には、図４の情報に加え、各資源をアクセス許可する計算機名が登録されている。これは、複数の携帯情報端末１１からのアクセス要求に対処するためである。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ２１７に記録される（ステップＳ３６，３７）。

【００４１】５．また、アクセス要求を許可した場合には、サーバ計算機２１は、要求元の携帯情報端末１１に資源を渡す（ステップＳ３８）。

６．携帯情報端末１１は、サーバ計算機２１からのアクセス許可の返答に応じて、サーバ計算機２１から渡された資源をユーザに渡す（ステップＳ２５）。

【００４２】この様に、実施形態２においても、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加されているので、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。また、サーバ計算機２１の利用によって、アクセス可能な資源の量を増やすことができる。さらに、ユーザが直接利用する携帯情報端末１１の構成が簡素化されるため、小型化／軽量化／低コスト化が図れ、個人が携帯ＰＣを持ち歩くといったようなモーバイルコンピューティングに最適なアクセス制御システムを構築できる。

【００４３】次に、図９乃至図１１を参照して、この発明の第３実施形態を説明する。図９には、この発明の第３実施形態に係るアクセス制御システムの実現形態が示されている。第３実施形態のアクセス制御システムは、サーバ計算機２１から渡された各種資源１３５を保持し、その管理および運用を行うキャッシュ管理部１３３が携帯情報端末１１に設けられており、ユーザから要求された資源が携帯情報端末１１内にある場合にはその資源に対するアクセス要求の可否判定を携帯情報端末１１のアクセス可否判定部１３４で行い、ユーザから要求された資源が携帯情報端末１１内にない場合にはその資源に対するアクセス要求の可否判定をサーバ計算機２１のアクセス可否判定部２２４で行う構成である。

【００４４】次に、図１０および図１１のフローチャートを参照して、図９のアクセス制御システムの動作について説明する。ここで、図１０は携帯情報端末１１側の処理を示し、図１１はサーバ計算機２１側の処理を示している。

【００４５】ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。

１．携帯情報端末１１のアクセス制御システムは、ユーザがある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップＳ４１）、以下のアクセス制御動作を行う。

【００４６】２．すなわち、まず、携帯情報端末１１のユーザ識別認証部１３１はユーザを特定し、場所識別認証部１３２はユーザのいる場所のセキュリティレベルを特定して、結果をアクセス可否判定部１３４に渡す（ステップＳ４２，Ｓ４３）。

【００４７】３．アクセス可否判定部１３４は、対象資源が携帯情報端末１１上にあるか否かをキャッシュ管理部１３３に問い合わせ、キャッシュ検索を実行させる（ステップＳ４４）。

【００４８】４．対象資源が携帯情報端末１１上にあった場合、アクセス可否判定部１３４は、ユーザ、場所のセキュリティレベル、対象資源の情報を元に、サーバ計算機２１から以前に渡された資源に関するアクセス制御リスト１３６をサーチし、アクセス要求の許可／非許可を判定する（ステップＳ４５）。アクセス制御リスト１３６は、図４のようなデータ構造を持つ。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ１３７に記録される（ステップＳ４６，Ｓ４７）。また、アクセス要求を許可した場合には、アクセス制御システムは、ユーザに対して要求された資源を渡す（ステップＳ４８）。

【００４９】５．対象資源が携帯情報端末１１上になかった場合には、携帯情報端末１１のアクセス可否判定部１３４は、ユーザ、場所のセキュリティレベル、対象資源の情報を、リモートマシンであるサーバ計算機２１に

アクセス要求として送る（ステップＳ４９）。

【００５０】６．サーバ計算機２１はそのアクセス要求に応答してイベント待ち状態から抜け（ステップＳ６１）、そして、計算機識別認証部２２２は、要求元の計算機を特定し、結果をアクセス可否判定部２２４に渡す（ステップＳ６２）。また、ユーザ情報検証部２２１と場所情報検証部２２２は、携帯情報端末１１から送られてきた情報が正しいかを検証し、結果をアクセス可否判定部２２４に渡す（ステップＳ６３，Ｓ６４）。

【００５１】７．アクセス可否判定部２２４は、ユーザ、アクセス場所のセキュリティレベル、要求元の計算機、対象資源の情報を元に、アクセス制御リスト２２６をサーチし、アクセス要求の許可／非許可を判定する（ステップＳ６５）。アクセス制御リスト２２６には、図４の情報に加え、各資源をアクセス許可する計算機名が登録されている。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ２１７に記録される（ステップＳ６６，６７）。

【００５２】８．また、アクセス要求を許可した場合には、サーバ計算機２１は、要求元の携帯情報端末１１に資源を渡す（ステップＳ６８）。

９．携帯情報端末１１は、サーバ計算機２１より資源とそれに関するアクセス制御リストが渡された場合は、キャッシュ管理部１３３がその資源およびアクセス制御リストを携帯情報端末１１内に記憶した後、その資源をユーザに渡す（ステップＳ５０，Ｓ５１）。

【００５３】この様に、実施形態３においても、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加されているので、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。また、一度利用した資源は、携帯情報端末１１上に保存されるので、一般的に通信時間／通信コストのかかるサーバへ計算機２１の問い合わせ回数を減らすことができる。

【００５４】なお、以上の実施形態１～３では、場所識別子認証部１１２，１２２，１３２が図２の発信器１００を用いてアクセス場所の情報セキュリティーレベルを特定する場合を説明したが、場所の識別子とその場所のセキュリティーレベルとの対応関係を示すテーブルを用意しておけば、場所識別子認証部１１２，１２２，１３２をそれぞれアクセス場所の識別子だけを検知するだけの構成にしても、アクセス場所に応じたアクセス制御を行うことができる。

【００５５】

【発明の効果】以上説明したように、この発明によれば、アクセス制御の基準に、アクセス要求してきた「場所」の情報を追加することで、制御が細かくできるようになり、モーバイルコンピューティングなど、不特定の場所からの各種資源へのアクセスといった状況においても、セキュリティを確保しながら、ユーザの利便を増すことが可能となる。

【図面の簡単な説明】

【図１】この発明の第１の実施形態に係るアクセス制御システムが適用されるモーバイルコンピューティングシステム全体の構成を示すブロック図。

【図２】同第１実施形態のアクセス制御システムにおけるアクセス場所に関する識別および認証処理の原理を説明するための図。

【図３】同第１実施形態のアクセス制御システムで使用されるセキュリティーレベル発信器から発生されるセキュリティーレベル信号の内容とセキュリティレベルの高低との対応関係を説明するための図。

【図４】同第１実施形態のアクセス制御システムで使用されるアクセス制御リストの構成を示す図。

【図５】同第１実施形態のアクセス制御システムのアクセス制御処理の手順を示すフローチャート。

【図６】この発明の第２の実施形態に係るアクセス制御システムの構成を示すブロック図。

【図７】同第２実施形態のアクセス制御システムのアクセス制御処理の手順の一部を示すフローチャート。

【図８】同第２実施形態のアクセス制御システムのアクセス制御処理の手順の残りの一部を示すフローチャート。

【図９】この発明の第３の実施形態に係るアクセス制御システムの構成を示すブロック図。

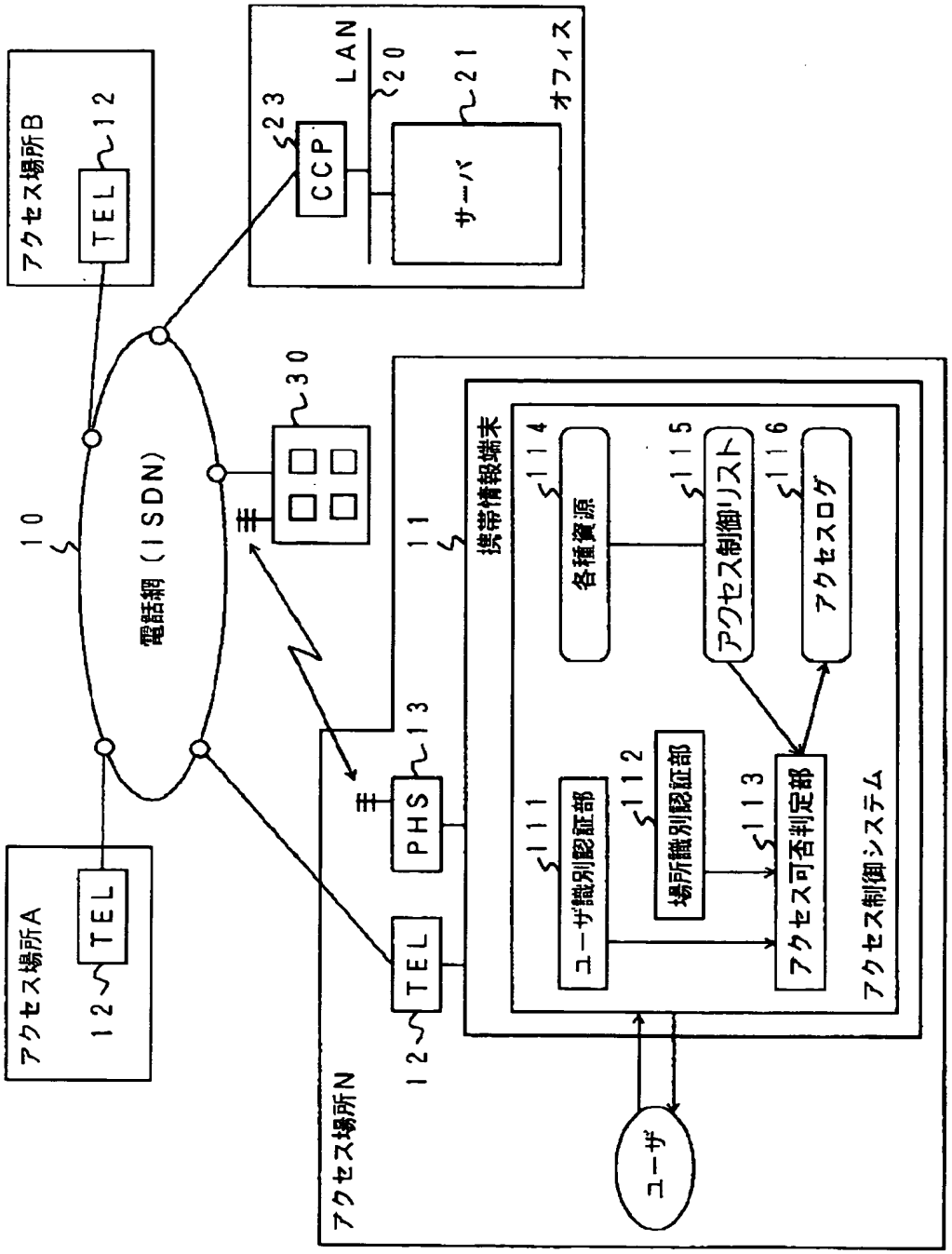
【図１０】同第３実施形態のアクセス制御システムのアクセス制御処理の手順の一部を示すフローチャート。

【図１１】同第３実施形態のアクセス制御システムのアクセス制御処理の手順の残りの一部を示すフローチャート。

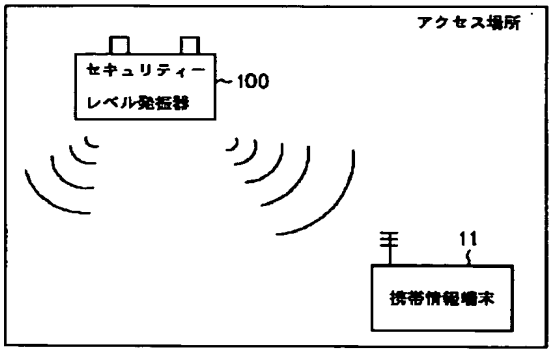
【符号の説明】

１１…携帯情報端末、２１…サーバ計算機、１１１，１２１，１３１…ユーザ識別認証部、１１２，１２２，１３２…アクセス場所識別認証部、１１３，１３４，２１４，２２４…アクセス可否判定部、１１５，１３６，２１６，２２６…アクセス制御リスト。

【図1】


アクセス場所B
TEL
12
オフィス
CCP
23
LAN
20
21
サーバ
10
電話網（ISDN）
30
11
携帯情報端末
各種資源
114
アクセス制御リスト
115
アクセスログ
116
PHS
13
ユーザ識別認証部
111
場所識別認証部
112
アクセス可否判定部
113
アクセス制御システム
アクセス場所A
アクセス場所N
ユーザ

【図２】



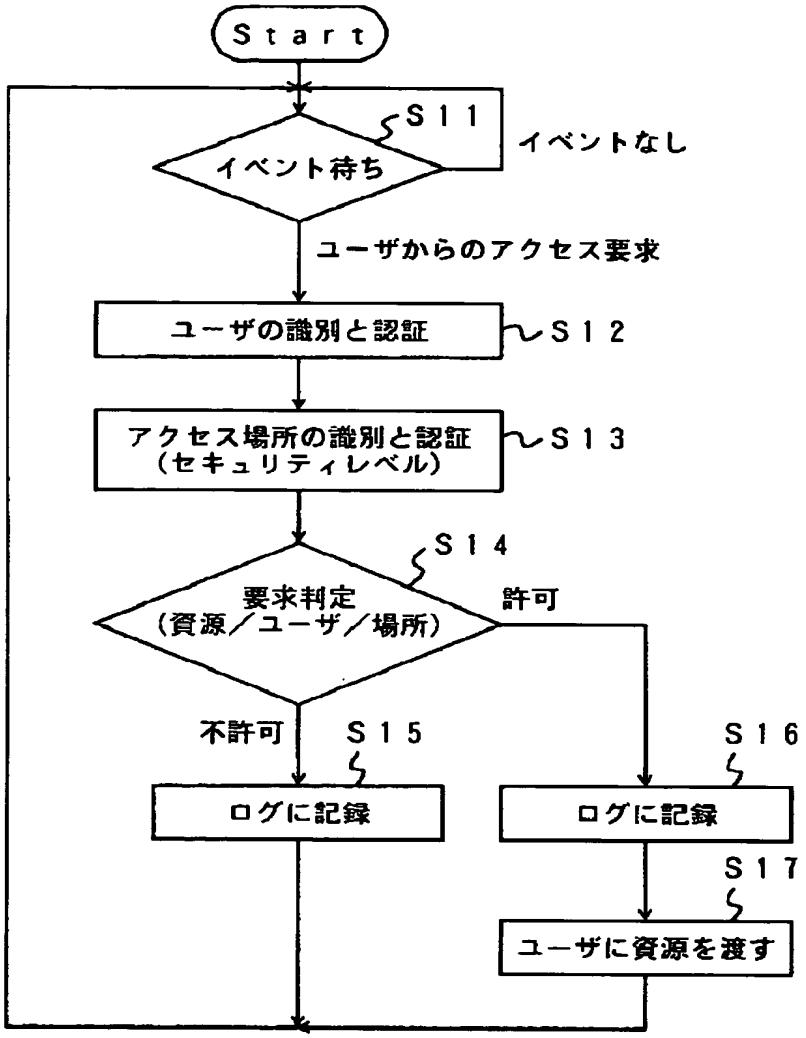
【図３】

セキュリティーレベル識号	セキュリティーレベル
A	高
B	
C	
D	
E	
F	低

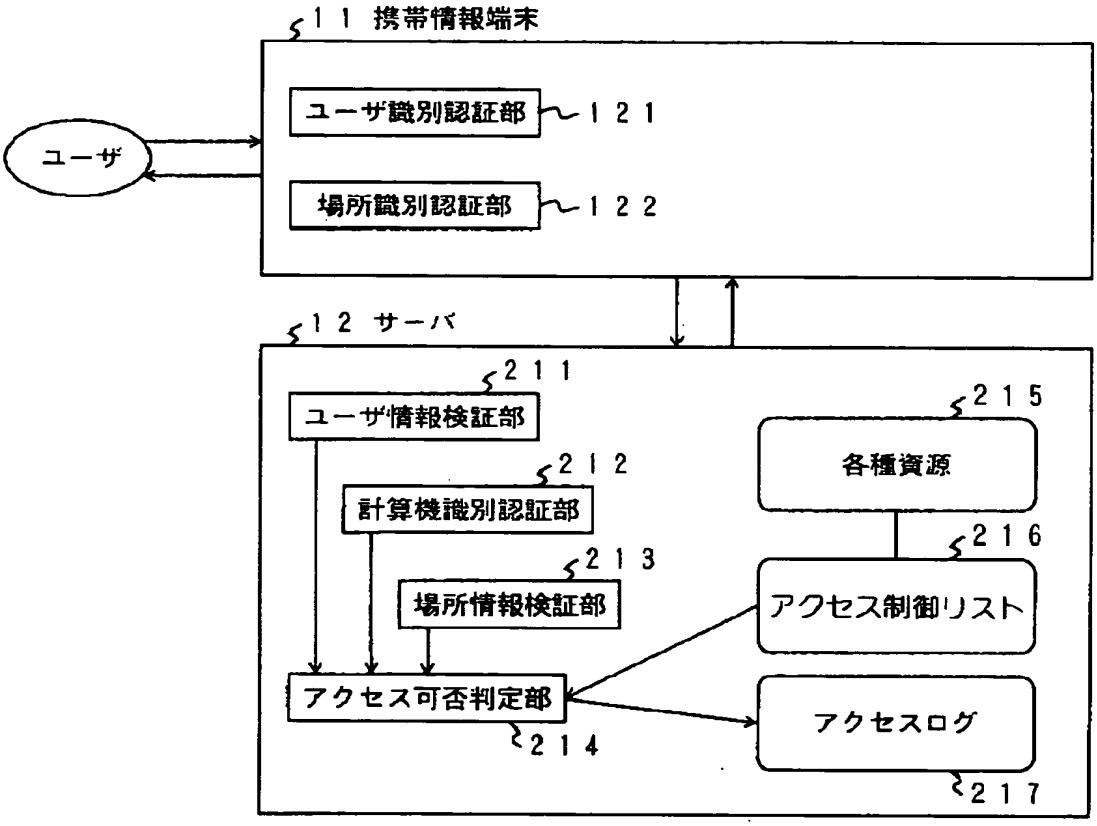
【図４】

資　源	ユーザ名／グループ名	セキュリティーレベル
データファイルA		A
	⋮	
データファイルB		C
⋮	⋮	⋮

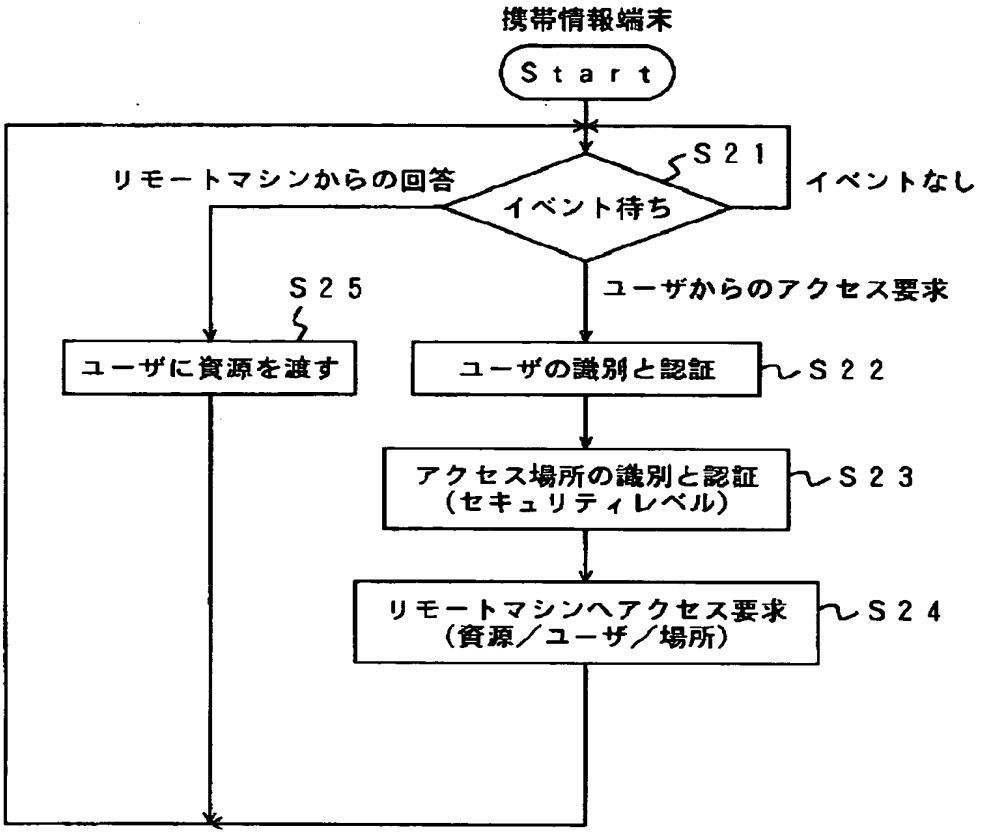
【図５】


Ｓｔａｒｔ
Ｓ１１
イベント待ち
イベントなし
ユーザからのアクセス要求
ユーザの識別と認証
Ｓ１２
アクセス場所の識別と認証
（セキュリティレベル）
Ｓ１３
Ｓ１４
要求判定
（資源／ユーザ／場所）
許可
不許可
Ｓ１５
ログに記録
Ｓ１６
ログに記録
Ｓ１７
ユーザに資源を渡す

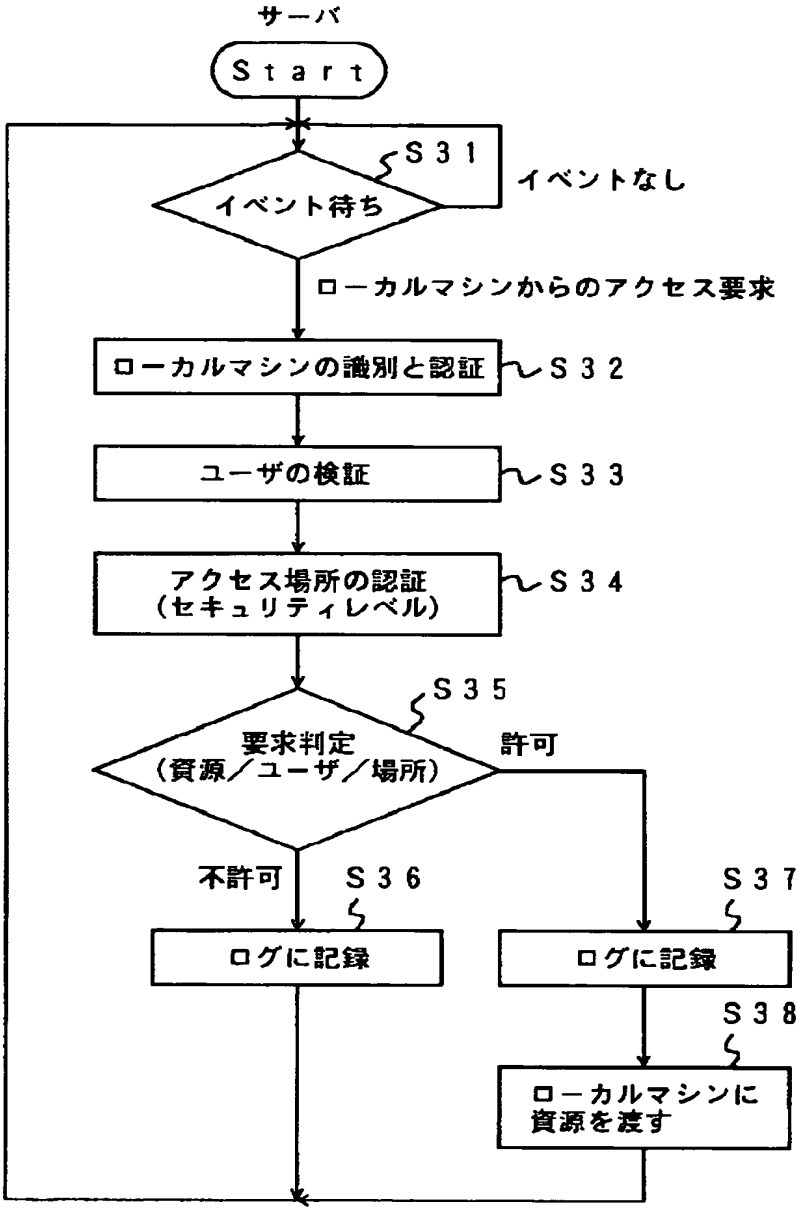
【図６】


１１ 携帯情報端末
ユーザ識別認証部
１２１
ユーザ
場所識別認証部
１２２
１２ サーバ
２１１
ユーザ情報検証部
２１５
各種資源
２１２
計算機識別認証部
２１６
２１３
場所情報検証部
アクセス制御リスト
アクセス可否判定部
アクセスログ
２１４
２１７

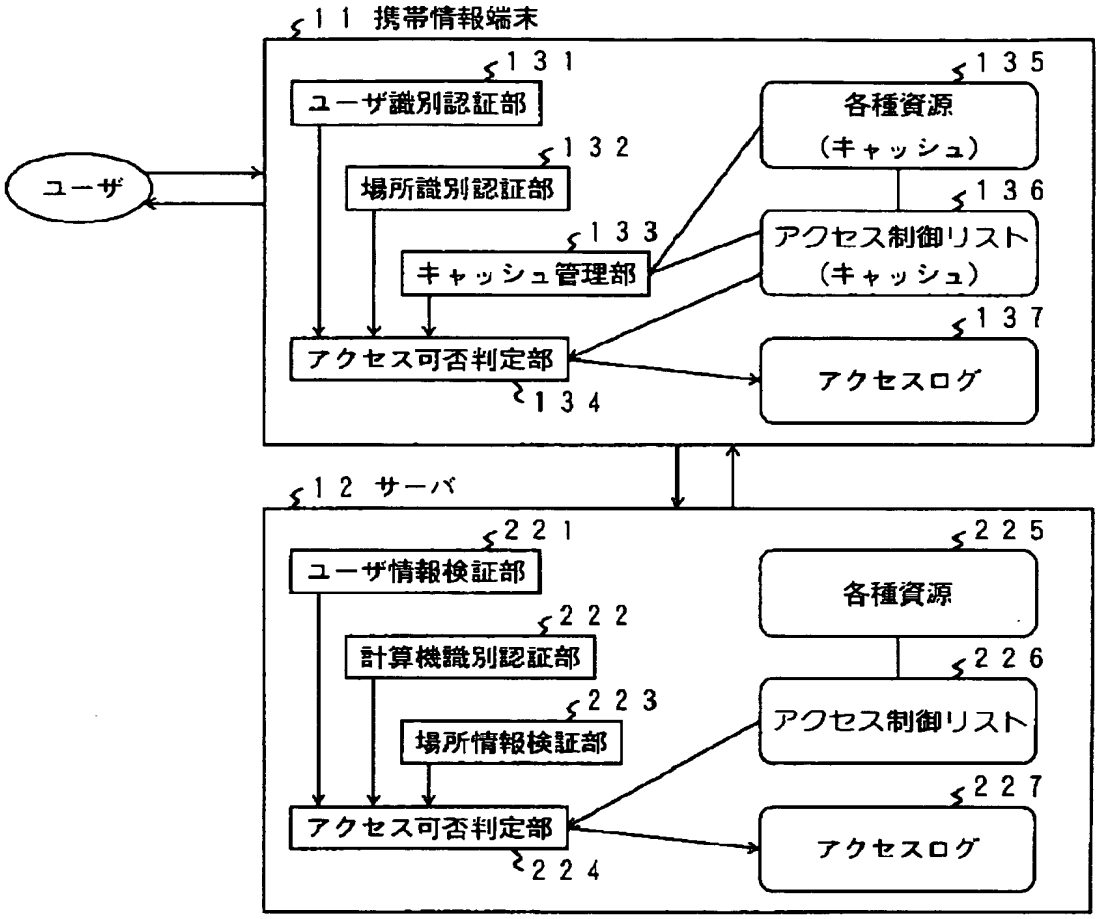
【図７】


携帯情報端末
Ｓｔａｒｔ
Ｓ２１
イベント待ち
イベントなし
リモートマシンからの回答
ユーザからのアクセス要求
Ｓ２５
ユーザに資源を渡す
ユーザの識別と認証
Ｓ２２
アクセス場所の識別と認証
（セキュリティレベル）
Ｓ２３
リモートマシンへアクセス要求
（資源／ユーザ／場所）
Ｓ２４

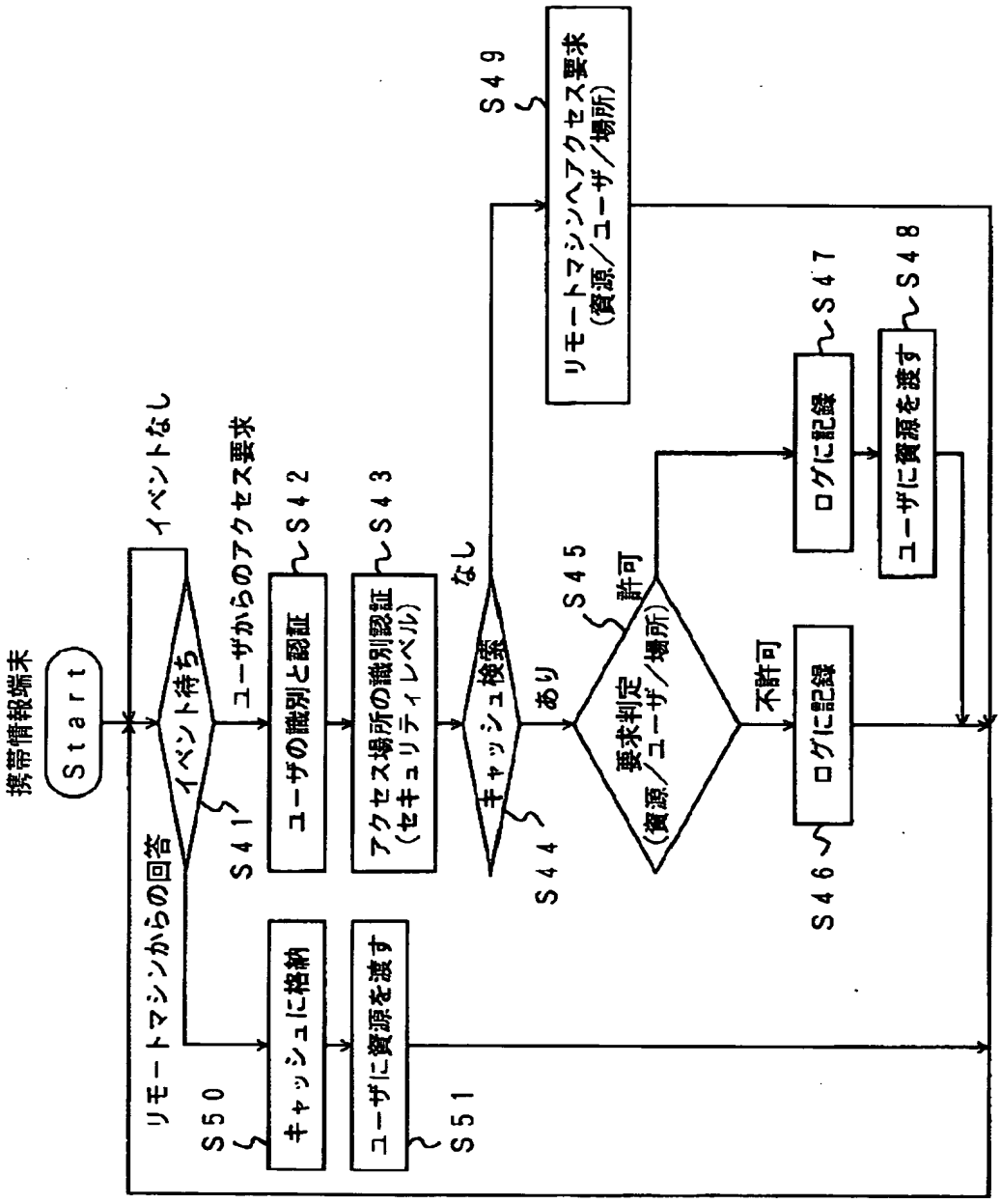
【図８】


サーバ
Ｓｔａｒｔ
Ｓ３１
イベント待ち
イベントなし
ローカルマシンからのアクセス要求
ローカルマシンの識別と認証
Ｓ３２
ユーザの検証
Ｓ３３
アクセス場所の認証
（セキュリティレベル）
Ｓ３４
Ｓ３５
要求判定
（資源／ユーザ／場所）
許可
不許可
Ｓ３６
Ｓ３７
ログに記録
ログに記録
Ｓ３８
ローカルマシンに
資源を渡す

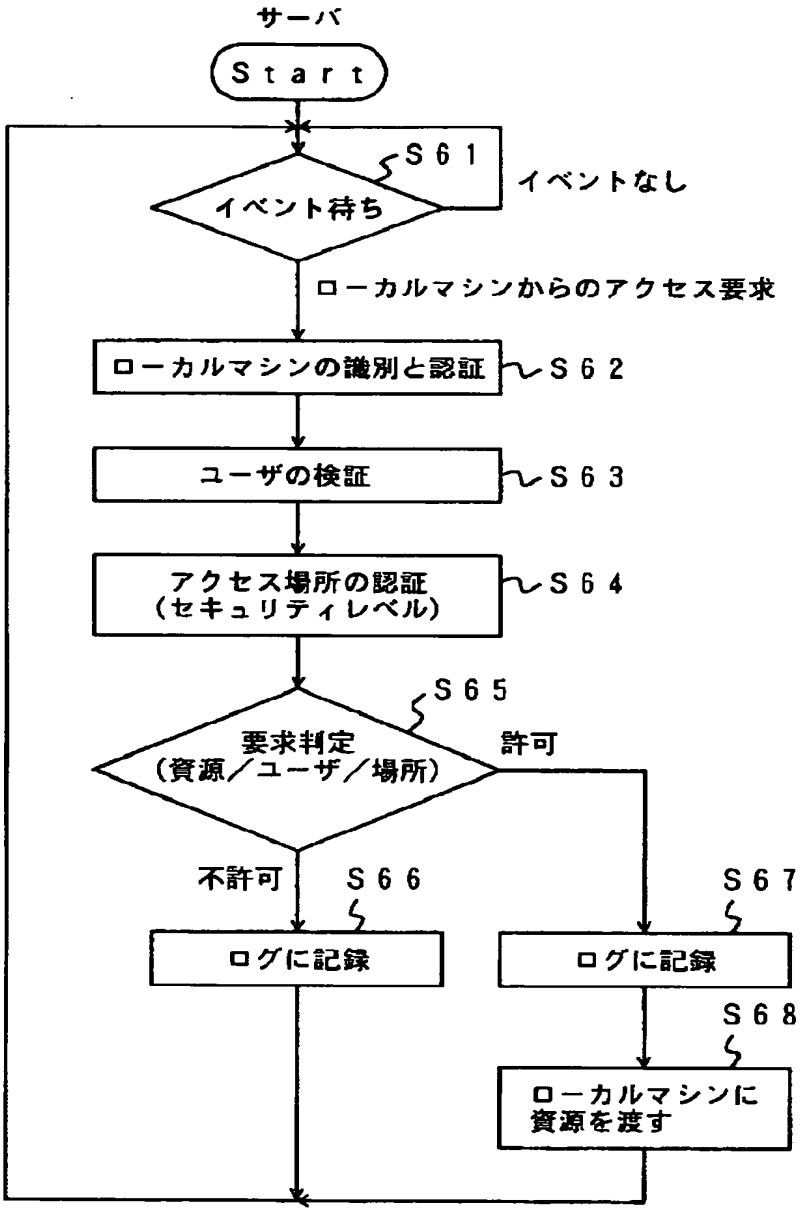
【図９】


１１ 携帯情報端末
１３１
ユーザ識別認証部
１３２
場所識別認証部
１３３
キャッシュ管理部
１３４
アクセス可否判定部
１３５
各種資源
（キャッシュ）
１３６
アクセス制御リスト
（キャッシュ）
１３７
アクセスログ
ユーザ
１２ サーバ
２２１
ユーザ情報検証部
２２２
計算機識別認証部
２２３
場所情報検証部
２２４
アクセス可否判定部
２２５
各種資源
２２６
アクセス制御リスト
２２７
アクセスログ

【図１０】


携帯情報端末
Start
リモートマシンからの回答
イベント待ち
イベントなし
S41
ユーザからのアクセス要求
S42
ユーザの識別と認証
S43
アクセス場所の識別認証
(セキュリティレベル)
S44
キャッシュ検索
なし
あり
S45
要求判定
(資源／ユーザ／場所)
許可
不許可
S46
ログに記録
S47
ユーザに資源を渡す
S48
S49
リモートマシンへアクセス要求
(資源／ユーザ／場所)
S50
キャッシュに格納
S51
ユーザに資源を渡す

【図１１】


サーバ
Ｓｔａｒｔ
Ｓ６１
イベント待ち
イベントなし
ローカルマシンからのアクセス要求
ローカルマシンの識別と認証
Ｓ６２
ユーザの検証
Ｓ６３
アクセス場所の認証
（セキュリティレベル）
Ｓ６４
Ｓ６５
要求判定
（資源／ユーザ／場所）
許可
不許可
Ｓ６６
ログに記録
Ｓ６７
ログに記録
Ｓ６８
ローカルマシンに
資源を渡す